NFIPM Section 23 (U) Threats to the National Information Infrastructure - Counterterrorism/Counterintelligence (TNII - CT/CI) Computer Intrusion (288J and 288B Subclassifications)

(For more information regarding the 288 classification and subclassifications, see EC from Cyber to Records Management dated 11/15/2005, 319W-HQ-A1487698 serial 27.)

Section 23-01 (U) Threats to the National Information Infrastructure (TNII) Investigations

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 08/09/2010.

Eff. Date: 08/09/2010

Section 23-02 (U) Lead Agencies

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 08/09/2010.

Eff. Date: 08/09/2010

Section 23-03 (U) The National Coordinator for Security, Infrastructure Protection and Counterterrorism

A. (U) The National Coordinator participates as a full member of Deputies or Principals Committee meetings when they are convened to consider infrastructure issues; and he/she reports to the President through the Assistant to the President for National Security Affairs.
B. (U) The National Coordinator ensures interagency coordination for policy development and implementation; and he/she chairs the Critical Infrastructure Coordination Group. See: id., Section VI(3) and Annex A, p. 11.

EFFDATE: 04/29/2002 MCRT# 1262 Div. CY Cav: SecClass: Unclassified

Section 23-04 (U) Interagency Groups

A. (U) The National Infrastructure Protection Center (NIPC) serves as the national critical infrastructure threat assessment, warning, vulnerability and law enforcement investigation and response entity. It consists of investigators from Lead Agencies who are experienced in computer crimes and infrastructure protection.
1. In the event of a foreign threat or attack, depending on the nature and level of the threat or attack; protocols established between DOJ/FBI, [redacted] and the ultimate decision of

b7E

the President, the NIPC may be may be placed in a direct support role [redacted] or the USIC. See: id., Annex A, p. 12.

B. (U) The Critical Infrastructure Coordination Group is a forum for the convening of Function Coordinators and Sector Coordinators. Where appropriate, the Group is assisted by the Security Policy Board, the Security Policy Forum and the National Security and Telecommunications and Information Systems Security Committee. See: id., Section VI(3).

C. (U) The National Plan Coordination staff serves to integrate the various sector plans into a National Infrastructure Assurance Plan, and to coordinate analyses of the U.S. Government=s own dependencies on critical infrastructures. See: id., Annex A, p. 11. b7E

(U) D. (U) The Terrorist Incident Working group consists of representatives from DOS, Treasury, DOD, DOJ, CIA, JCS, FBI, the Office of the Vice President, the NSC staff and such other departments and agencies as may be necessary. This Group is activated by the Assistant to the President for National Security Affairs, or at the request of any of its members; and it remains convened for the duration of terrorist incidents. See: National Security Decision Directive Number 207, p.3.

(U) [redacted]

(U) [redacted]

(U) [redacted]

(U) [redacted]

(U) I. (U) The Counterterrorism Security Group coordinates counterterrorism issues and reviews ongoing crises operations. See: Presidential Decision Directive/NSC-62, p.13.

EFFDATE: 04/29/2002 MCRT# 1262 Div. CY Cav: SecClass: Secret

Section 23-05 (U) Cyber Division - Mission

A. (U) Cyber Division (CyD) is dedicated to applying the highest level of technical capital toward combating cyber-based terrorism, hostile intelligence operations conducted over the Internet, and cybercrime. By aggregating its cyber-centered investigations within one division, the FBI is able to more effectively and efficiently identify, investigate, and neutralize cyber threats. As the nation's cyber dependency becomes even more profound, the Cyber Division will continue to be the vanguard of security for its citizens and its critical infrastructures.

B. (U) The CyD, Computer Intrusion Section (CIS) is charged with providing administrative and operational support and guidance for computer intrusion investigations, including Threats to the

National Information Infrastructure - Counterterrorism / Counterintelligence (TNII-CT/CI) matters and criminal matters. Additionally, CIS coordinates computer intrusion investigations by various criminal investigative and intelligence components of the Federal Government.

EFFDATE: 01/17/2003 MCRT# 1273 Div. CY Cav: SecClass: Unclassified

Section 23-06 (U) TNII Matters - Investigative Guidance

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 08/09/2010.

Eff. Date: 08/09/2010

Section 23-07 (U) The 288 Subclassification

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 08/09/2010.

Eff. Date: 08/09/2010

Section 23-08 288A - Computer Intrusion - Criminal

A. (U) The 288A Subclassification should be utilized upon the receipt of a computer intrusion report and the initiation of a criminal investigation. Examples of criminal computer intrusions include Denial of Service attacks, network intrusions resulting in theft of proprietary or customer information, computer virus attacks which disrupt or destroy data contained on computers, and insertion of malicious computer code which impedes or impairs computer data.
B. (U) As stated in the Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Domestic Security/Terrorism Investigations, "All investigations of crime or crime-related activities shall be undertaken in accordance with one or more of these guidelines." In short, criminal investigative authorities, as set forth in these guidelines, are utilized during investigations of criminal activity, suspected criminal activity, in violation of federal criminal statutes, i.e. the United States Code.
C. (U) Guidance regarding the conduct and reporting of 288A matters can be found in the Manual of Investigative and Operational Guidelines (MIOG), Part 1, Section 288.

EFFDATE: 01/17/2003 MCRT# 1273 Div. CY Cav: SecClass: Unclassified

Section 23-09 (U) 288B - Threats to the National Information Infrastructure - Counterintelligence

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 08/09/2010.

Eff. Date: 08/09/2010

Section 23-10 (U) 288C-H - Technical Assistance Matters

A. The 288C-H classifications involve Computer Intrusion Squad technical expert assistance to other program's computer-facilitated crime. Computer Intrusion Squad members should [redacted] noncomputer intrusion matters as follows: b7E
288C Technical Assistance to WCC Program
288D Technical Assistance to VCMO Program
288E Technical Assistance to OC/DP
288F Technical Assistance to CI
288G Technical Assistance to DT Program
288H Technical Assistance to CR Program
288L Technical Support to IT Program

(U) Section 23-11 (S) National HUMINT Collection Directive (NHCD) - The 288I Classification

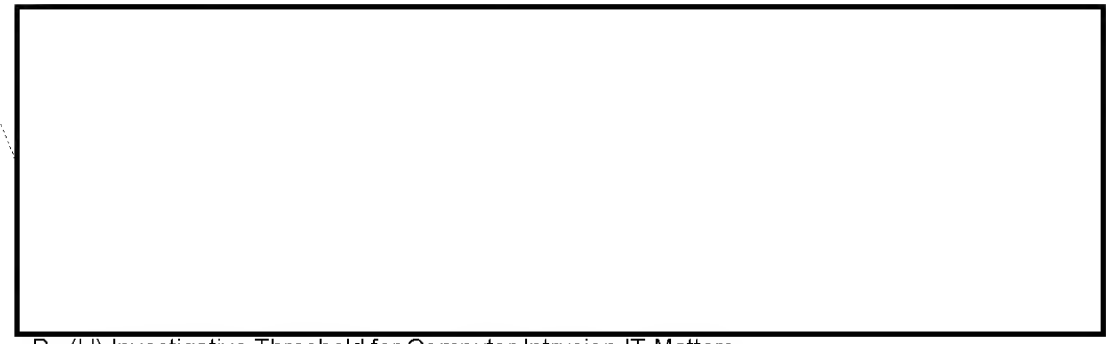
Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 08/09/2010.

Eff. Date: 08/09/2010

Section 23-12 (U) 288J - Computer Intrusions -International Terrorism (IT) Matters

A. General
1. (U) Computer Intrusions IT investigations are national security investigations in support of the FBI's priority to protect the United States from terrorist attack with the goal of preventing, disrupting, and defeating terrorist operations before they occur. Computer Intrusion IT investigations may often involve, but are not limited to, investigations of person, groups or organizations, who are or may be engaged in activities targeting the national information infrastructure for, on behalf of, or in coordination with a foreign power, or in activities of international terrorism. The purpose of these investigations is to collect information and engage in activities to detect and counteract foreign power sponsored or coordinated international terrorism threats, and clandestine or illegal activities directed against the national security of the United States.
(U) 2. ~~(S//NF)~~ Pursuant to Part I.A.1. of the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSIG), the Attorney General has authorized the FBI to conduct investigations to obtain information concerning or to protect against threats to national security, including investigations of crimes involved in or related to the national security, as provided in Part II and V of the NSIG, to include international terrorism and foreign computer intrusions Does part ii and V state this verbatim?.
a. Field offices should aggressively pursue Computer Intrusion IT investigations and should develop proactive operations consistent with the NSIG and in consultation with the Cyber Division (CyD). The CyD, in coordination with the Office of Intelligence and Policy Review (OIPR), Department of Justice, is fully engaged to support FBI counterterrorism investigations.
(U) 3. ~~(S//NF)~~ The CyD will coordinate with the Counterterrorism Division (CTD), as appropriate, at a program level. Field Office Cyber or Computer Intrusion squads should coordinate Computer Intrusion IT investigations with the appropriate CTD squad at the field level.

(S)



b1

B. (U) Investigative Threshold for Computer Intrusion IT Matters

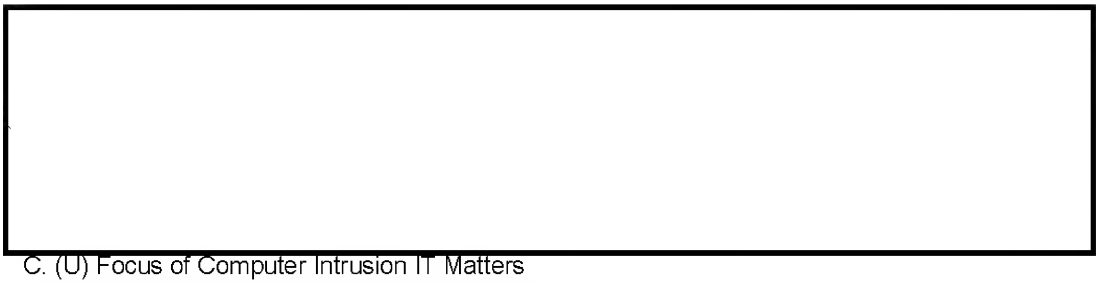
1. (U) The Computer Fraud and Abuse Act, as amended (the National Information Infrastructure Protection Act of 1996), is the principal federal statute that predicates computer intrusion investigations. The amended statute addresses the central tenets of computer and information system security, i.e., protecting the confidentiality, integrity, and availability of data and systems.

2. (U) Any investigation involving this violation could have national level consequences. However, field offices should closely monitor and especially focus on the following situations:

(S)

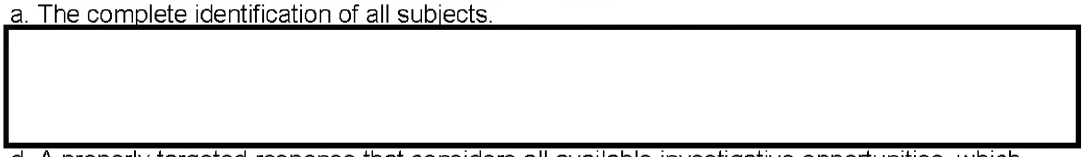
b1
b7E

(S)



b1

C. (U) Focus of Computer Intrusion IT Matters
1. (U) Computer Intrusion IT investigations must focus on:
a. The complete identification of all subjects.



b7E

d. A properly targeted response that considers all available investigative opportunities, which includes criminal prosecution. Because of the potential for eventual criminal prosecution, Computer Intrusion IT investigations should be conducted in a manner that preserves this option whenever possible.
D. (U) Significant Legal Matters
1. (U) Significant legal developments after September 11, 2001 important to Computer Intrusion IT investigations that affected IT investigations include:
(U) a. ~~(S)~~ The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection, effective October 31, 2003.
b. "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001" (USA PATRIOT Act), effective October 26, 2001; USA Patriot Improvement and Reauthorization Act of 2005; USA Patriot Act Additional Reauthorizing Amendments Act of 2006.
c. "Intelligence Sharing Procedures for Foreign Intelligence and Foreign Counterintelligence Investigations Conducted by the FBI," issued on March 6, 2002 by the Department of Justice (DOJ).
d. Foreign Intelligence Surveillance Court of Review's opinion issued on November 18, 2002, In re Sealed Case, 310 F.3d 717 (FISCR 2002).

Section 23-13 (U) 288J - Authorities, Procedures, and Requirements in Computer Intrusion IT Matters

A. (U) Computer Intrusion IT investigative Authorities and Standards
1. (U) The FBI shall conduct its Computer Intrusion IT investigations in compliance with the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSIG), which were issued October 31, 2003. The general objective of the NSIG is the full utilization of all authorities and investigative techniques, consistent with the Constitution and laws of the United States, so as to protect the United States and its people from terrorism and other threats to the national security.
2. (U) In addition to the NSIG, the FBI shall conduct its Computer Intrusion IT investigations in compliance with the Constitution and all applicable statutes, executive orders, DOJ regulations and policies, and other Attorney General guidelines.
3. (U) FBI Headquarters will be the national program manager and office of origin for all Foreign Terrorist Organizations designated by the U.S. Secretary of State. Field offices direct investigations on the activities of these organizations only within their respective areas of responsibility.

B. Procedural Requirements in Computer Intrusion IT matters

1. (U) There are three levels of investigative activity outlined in the NSIG for the conduct of IT investigations: Threat Assessments, Preliminary Investigations, and Full Investigations.

2. (U) A Computer Intrusion IT investigation in the 288J classification must be initiated when investigative steps are taken by the investigative personnel involved in either a Preliminary or Full investigation.

a. All investigative cases on individuals, groups, or organizations in the 288J classification must be characterized as either a Preliminary or Full Investigation. Control files are not investigative cases and thus are not designated as either a Preliminary or Full Investigation. b7E

b. Preliminary and Full Investigations of groups and organizations should focus on activities related to threats to the national security, not on unrelated First Amendment activities. Any information concerning a group or organization that is relevant to the investigation of a threat to the national security may be sought, including information on

(U) ×

(S)

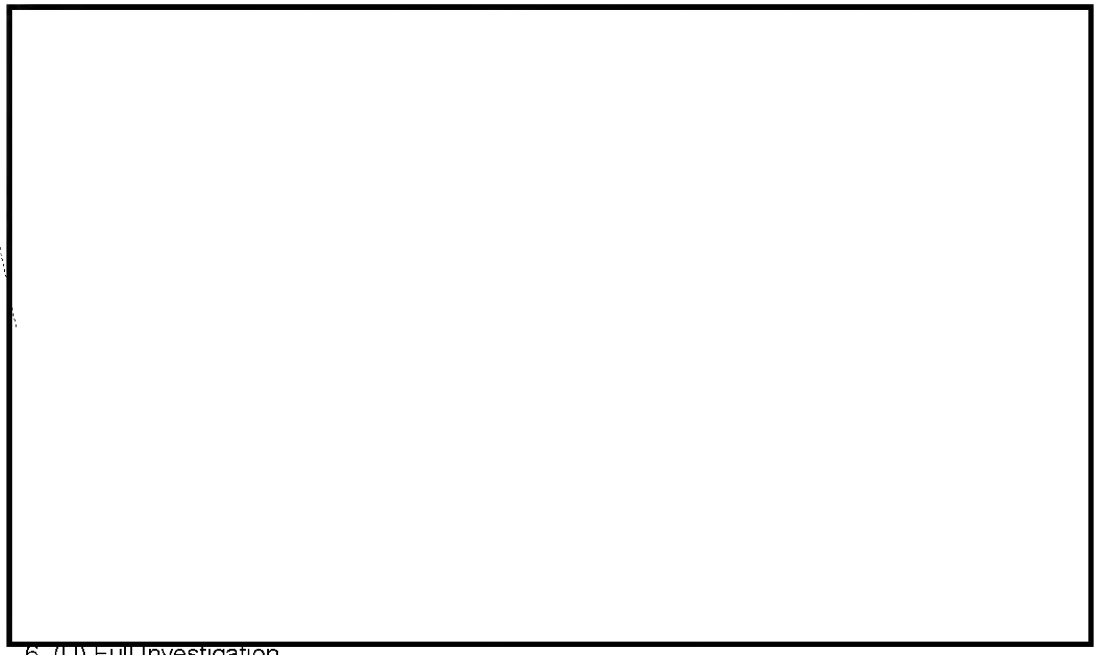
b1

(S) [redacted] b1

(U) (1) (S) A sensitive national security matter is defined in the NSIG as: "a threat to the national security involving the activities of an official of a foreign country other than a threat country, a domestic public official or political candidate, a religious or political organization or an individual prominent in such an organization, or news media, or any other matter which, in the judgment of the official authorizing an investigation, should be brought to the attention of FBI Headquarters and other Department of Justice officials."

(S) [redacted] b1

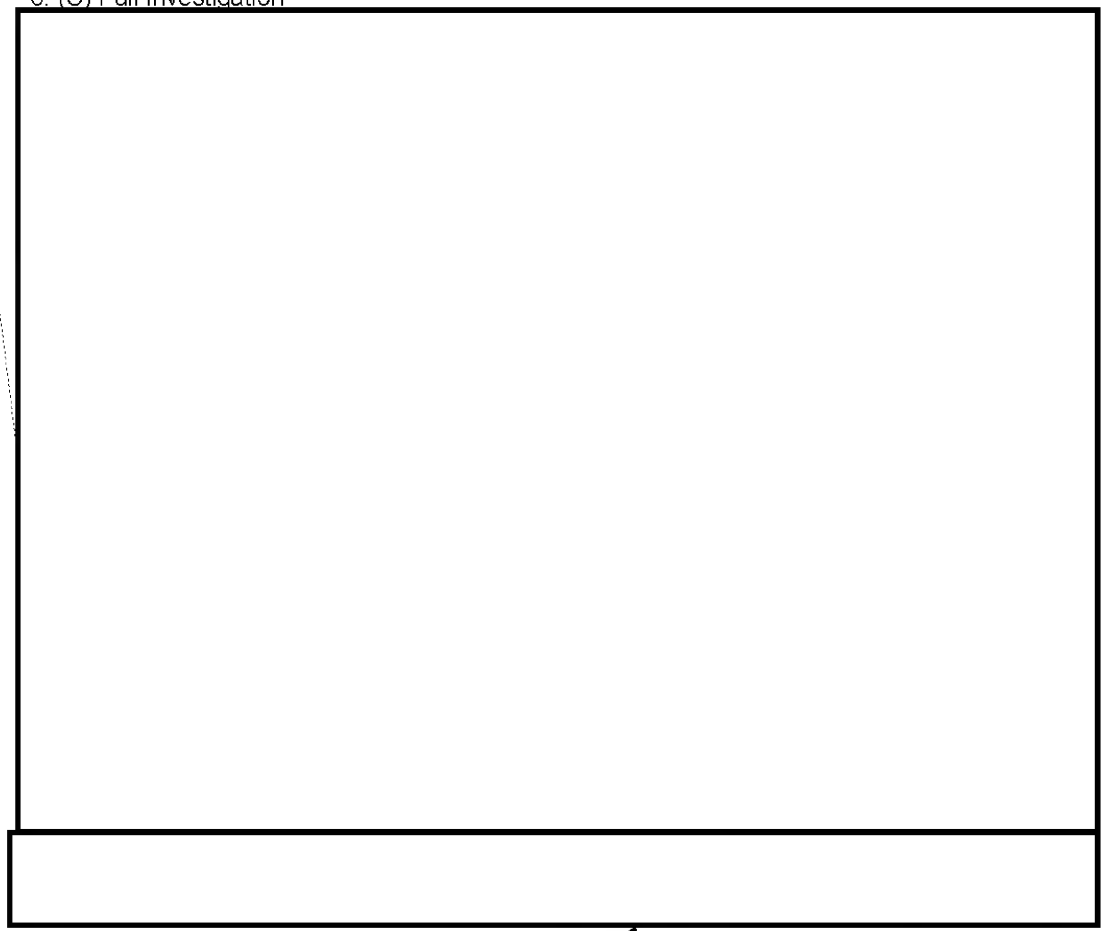
(S)



b1

6. (U) Full Investigation

(S)



b1

b1
Referral/Consult

(S) [redacted]

(U) (1) (S) A sensitive national security matter is defined in the NSIG as: "a threat to the national security involving the activities of an official of a foreign country other than a threat country, a domestic public official or political candidate, a religious or political organization or an individual prominent in such an organization, or news media, or any other matter which, in the judgment of the official authorizing an investigation, should be brought to the attention of FBI Headquarters and other Department of Justice officials."

(S) [redacted] b1

(U) h. (S/NF) The Office of Origin is determined by the residence, location or destination of the subject of the investigation. If special circumstances exist, for example, [redacted] b7E origin may be assumed by the office having the most compelling investigative interest. Uncertainties regarding the appropriate Office of Origin shall be resolved by FBIHQ.

(S) [redacted] b1

(U) 5. (~~S~~) A sensitive national security matter is defined in the NSIG as: "a threat to the national security involving the activities of an official of a foreign country other than a threat country, a domestic public official or political candidate, a religious or political organization or an individual prominent in such an organization, or news media, or any other matter which, in the judgment of the official authorizing an investigation, should be brought to the attention of FBI Headquarters and other Department of Justice officials." b7E

(U) [redacted]

D. (U) Notification of Case Opening

(S) [redacted] b1

(S) [redacted] b1

F. (U) United States Person

1. (U) A United States Person is defined in the NSIG as one of the following:

a. an individual who is a United States citizen or an alien lawfully admitted for permanent residence;

b. an unincorporated association substantially composed of individuals who are United States person; or

c. a corporation incorporated in the United States.

2. (U) In the absence of information establishing otherwise, subjects are presumed to be U.S. Persons.

3. (U) A foreign power as defined in Part VIII.L.1.-3. of the NSIG is never to be considered a United States person, including any foreign government or component thereof, any faction of a foreign nation or nations not substantially composed of individuals who are United States persons, or any entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments.

G. (U [redacted]

1. (U) The notification requirements to CyD of the initiation of a new computer intrusion IT investigation, described above, do not obviate the need or negate the requirement to submit [redacted] b7E

H. Undercover Operations in Computer Intrusion IT matters

(U) 1. ~~(S//NF)~~ The use of undercover operations as an investigative technique in Computer Intrusion IT matters can be very productive. However, inherent in the use of such techniques are legal, operational and policy considerations. Guidelines set forth in Section 28, infra, of this manual are applicable to all Computer Intrusion IT undercover operations and should be utilized to efficiently establish and manage undercover operations.

I. Extraterritorial operations in Computer Intrusion IT matters

[redacted]

J. (U) Computer Intrusion IT matters and Criminal Programs
1. (U) An computer intrusion IT investigation might also impact criminal programs overseen by the Criminal Investigative Division (CID). In those instances, the appropriate CID unit should also be apprised of the investigation in the initial communication to CyD.
2. (U) Any investigation properly opened as an International Terrorism investigation after delineating specific facts clearly establishing a terrorism nexus, which also possesses a drug nexus, must be conducted not only in conformance with the NSIG, but also in accordance with existing guidelines as stated in MIOG, Part 1, Sections 245 and 281. Since the need for interagency coordination is particularly acute with regard to drug matters, the initial communication advising CyD of the computer intrusion IT case initiation must also be directed to the CID, Drug Section. If there is an international nexus, then a copy should also be directed to the appropriate Legal Attache for information.
K. (U) Case Title Examples

(S) [redacted] b1

4. (U) File numbers are unclassified. Case titles, except code word titles, are classified.

[redacted] b7E

[redacted] b7E

M. (U) Unaddressed Work
1. (U) There will be no unaddressed work within the Computer Intrusion IT program of any field office.
N. (U) Code Word Operations
1. (U) As appropriate, code word operations may be opened as Computer Intrusion IT investigations and conducted in accordance with a Preliminary Investigation or Full Investigation.
O. (U) Control and Administrative Files (See MAOP, Part 2, 2-4.1.2 and 2-4.1.5)
1. (U) Control files in the 288J classification (288J-FO-C) may be maintained by field offices. Control files are separate files established for the purpose of administering specific phases of an investigative matter or program and would not be considered a PI or FI. They are neither Preliminary nor Full Investigations and thus do not require [redacted]
2. (U) The 288J zero (288J-0) file may be utilized for material which does not require investigation, such as complaints that have been addressed, but were deemed not credible. Investigative leads cannot be set out of the 288J zero file.
P. (U) Sub-File Folders
1. (U) Routine Folders should be opened within the Computer Intrusion IT investigation in accordance with the standards outlined in MAOP, Part 2, 2-5.1. The list of approved folders includes:
1A 1A Section exhibits1B FD-192s (evidentiary bulkies)
1C FD-192s (nonevidence bulkies)
BC Background Information
CE Case Expenditures
ELA ELSUR Administrative
ELA1 ELSUR Original Logs
ELA1A ELSUR Copies and Logs
ELA1B ELSUR Transcripts
GJ Grand Jury Material
FISUR Physical Surveillance Logs
FF Forfeiture Matters
LAB Laboratory/Latent Reports
MC Mail Cover Materials
NC Newspaper Clippings (Press Releases)
SBP Subpoenas
TEL Telephone Subscriber and Toll Information
2. (U) In addition, Special Category Folders should be opened to organize specific investigative aspects of the case file. These folders should be created when information pertinent to the categories arises in the case. These special categories include:
a. FOREIGN Foreign Intelligence--for which permission would need to be granted from a host government prior to release to a third party (for example, the U.S. Attorney's Office).
b. OGA Intelligence from other government agencies--for which permission to disseminate would be required from the originating service (for example, the Naval Criminal Investigative Service).
c. TERRFIN Terrorist Financing--for information related to the funding of terrorism.
d. CRIMINAL For evidence and other information regarding investigation being pursued relating to specific acts of criminality.

(U) Q. (U) Approval Authority for Interviews in Computer Intrusion IT Investigations b1

(S) [redacted]

(S) [redacted] b1

R. (U) Classification

1. (U) It is important that investigators NOT overly classify information in terrorism investigations. Classification derives from the source of and method used to obtain the information, not the actual content of the information.

(U) [redacted] b7E

4. (U) Situations will often arise when classified information obtained during a Computer Intrusion IT investigation will be relevant to a criminal or civil proceeding. In this instance, a declassification review will be required, which, in turn, often requires a more fulsome translation effort than has been previously undertaken. FBI field offices must ensure the declassification review process is coordinated with the National Security Law Branch, Office of the General Counsel, and relevant CyD substantive units. If information was properly classified when placed in the case file, the review process will be much more efficient. If the litigation is a criminal case, further coordination may be required with the Department of Justice Criminal Division and relevant United States Attorney's Offices. Any information that should remain classified, and which is relevant to a criminal proceeding, will be managed under the Classified Information Procedures Act (CIPA). Classified information relevant to a civil proceeding may require a claim of State Secrets, which will require substantial involvement with the Civil Division of the Department of Justice and the personal intervention of the Attorney General (or other relevant Cabinet Officer).

S. (U) The Foreign Intelligence Surveillance Court (FISC)

(S) [redacted] b1

T. (U) Attorney-Client Privilege

(S) [redacted]

(S) [redacted] b1

U. (U) Violent Gang and Terrorist Organization File (VGTOF) and Terrorist Screening Center (TSC) Database

1. (U) Subjects of both Preliminary and Full Investigations must be entered into the Violent Gang and Terrorist Organization File (VGTOF) by completing an FD-930. In the FD-930, case Agents must make a recommendation [redacted] as to which databases the subject should be entered and a recommended Handling Code. Upon closing the Preliminary or Full Investigation, the case Agent shall remove subjects who no longer merit inclusion via form FD-930. b7E

2. (U) The "Miscellaneous" field on the FD-930 should include the case Agent's name and 24/7 contact number, the subject's USPER status and country of citizenship, and any other pertinent information. CLASSIFIED INFORMATION MAY NOT BE LISTED IN THE "MISCELLANEOUS" FIELD.

3. (U) The databases into which a subject can be entered will be listed in the FD-930, but they include the Violent Gang and Terrorist Organization File (VGTOF), TSA No Fly or TSA Selectee lists, Treasury Enforcement Communications Systems (TECS), and Consular Lookout and Support System (CLASS) for non-USPERs.

4. (U) The Handling Codes categories, and a description of each, will be listed in the FD-930.

V. (U) Information Sharing

1. (U) Information acquired during the course of a Computer Intrusion IT investigation should be shared as consistently and fully as possible among agencies with relevant responsibilities to protect the United States and its people from terrorism and other threats to national security, except as limited by specific statutory or policy constraints. Information may be disseminated to obtain information for the conduct of a lawful investigation by the FBI.

2. (U) The FBI (through CyD) shall keep the DOJ Criminal Division and the Office of Intelligence Policy and Review apprised of all information obtained through the conduct of Computer Intrusion investigations, except as limited by orders issued by the FISC, controls imposed by the originators of sensitive material, or restrictions established by the Attorney General or the Deputy Attorney General in particular cases.

3. (U) Subject to the conditions and terms described in the NSIG, relevant United States Attorney's Offices (USAOs) shall receive information and engage in consultations to the same extent as allowed the DOJ Criminal Division. Thus, the USAOs shall have access to information, shall be kept apprised of information necessary to protect national security and information concerning crimes, shall receive notices of the initiation of investigations and annual summaries, and shall have access to FBI files, to the same extent as the DOJ Criminal Division.

4. (U) Information disseminated to a USAO shall be disseminated only to the United States Attorney (USA) and/or any Assistant United States Attorneys (AUSAs) designated to the DOJ by the USA as points of contact to receive such information. The USA and AUSAs shall have appropriate security clearances and shall receive training in the handling of classified information and information derived from FISA, including training concerning restrictions on the use and dissemination of such information. A disseminable LHM is the appropriate method for presenting investigative findings to the Department of Justice. A copy of the LHM must also be directed to the appropriate CyD operational unit.

5. (U) Pursuant to the Attorney General's Intelligence Sharing Procedures, dated March 6, 2002, the FBI must keep a designated AUSA in the relevant USAO fully informed of all relevant foreign intelligence information, as well as evidence of any crime, including information and evidence obtained or derived from FISA, which arises during International Terrorism investigations. Information obtained or derived from FISA shall be marked as required in Title 50, United States Code, Sections 1806(b) and 1825(c).

6. (U) Foreign intelligence is defined in the NSIG as: "information relating to the capabilities, intentions, or activities of foreign powers, organizations, persons, or international terrorist activities."

W. Investigative Accomplishments (FD-542) in Computer Intrusion IT Matters
1. The FD-542 shall be utilized to capture statistical accomplishments not already captured in [redacted] which utilizes the FD-515 to capture data relative to traditional criminal statistical accomplishments. Although the method of capturing statistical accomplishments through the FD-515 [redacted] should be used when appropriate, the FD-542, through the FD-542 macro, shall be utilized to capture investigative accomplishment identified in Section 2-53, supra, relevant to national security and international terrorism investigations. b7E
X. Closing Computer Intrusion IT Matters
1. General
a. Prior to closing a Computer Intrusion IT investigation in the 288J classification, Field offices must ensure all reasonable investigative techniques have been exploited. By closing the investigation, the field office is affirming it has exhausted all reasonable and practical intelligence collection methods with respect to the investigation.
b. If the investigation has uncovered criminal violations of state or federal law, then a declination from the United States Attorney's Office must be received and documented within the investigative case file.
2. Closing Communication to FBIHQ
a. The closing communication will be sent to the CIS, CyD to the attention of the following:
(1) CyD Substantive section/unit
(2) CTD Substantive section/unit
(3) [redacted] b7E
(4) CT Analytical Section
(5) [redacted]
(6) Other sections or units, as appropriate
(7) Appropriate field office or Legal Attaché ("Legat"), if subject relocated
b. An FD-930 will be enclosed to remove or modify the entry in VGTOF.
c. The Details section of the closing communication will contain the following information:
(1) The type of investigation (i.e., Preliminary or Full)
(2) The date it was opened
(3) The date it was converted from a Preliminary Investigation to Full Investigation, if applicable
(4) If a Full Investigation, then the date and serial number of the most recent Annual Summary
(5) Whether the investigation involves a United States person
(6) An assessment of the extent to which the subject is (or members of the group are) aware of the terrorist aims of the foreign power
(7) Any sensitive national security matters, which is defined in the NSIG as "a threat to the national security involving the activities of an official of a foreign country other than a threat country, a domestic public official or political candidate, a religious or political organization or an individual prominent in such an organization, or news media, or any other matter which, in the judgment of the official authorizing an investigation, should be brought to the attention of FBI Headquarters and other Department of Justice officials."
(8) Name and all aliases of the subject and complete biographical information regarding the subject
(9) A summary of the investigation to include a list of the investigative techniques used, to include:

[redacted] b7E

[redacted]

b7E

(10) Whether the case was submitted to the United States Attorney's Office for criminal prosecution and result (indictment or declination); if there is a criminal declination, then the case Agent prepares a letter to the United States Attorney's Office that documents the declination, the letter must be uploaded into the case file, and referenced in the closing communication

3. Reason(s) for Closure of Case

a. Reason(s) for Closure of Case

(1) Subject was convicted

(a) Include details, to include jurisdiction, statute(s), and sentence

(2) Subject is incarcerated

(a) Include details, to include jurisdiction, statute(s), sentence, incarceration facility, projected release date

(b) Incarceration of a subject, by itself, does not meet the basic investigative standard which would merit an international terrorism case to be closed. Factors to be considered prior to closing include, but are not limited to:

[redacted]

(4) Subject is believed to have moved out of the field office's area of responsibility, but stayed within the USA

(a) include details, to include travel information, traveled with whom, location to which subject moved, and which field office has jurisdiction

(b) The change of residence of a subject, by itself, does not meet the basic investigative standard which would merit an IT case to be closed. If a subject has moved outside the area of

responsibility of a field office, then the current office of origin will prepare a communication transferring the investigation to the field office covering the subject's new residence. This communication will summarize the investigation to date and include action leads to both the new field office and the appropriate CyD substantive unit(s) to ensure a seamless and fluid transition between the two field offices.
(5) Subject is believed to be deceased
(a) Include details, to include basis for belief and circumstances of death
(6) Allegations against the subject are without merit
(a) Include details
4. (U) Leads
a. It is not possible to set leads, including information-only leads, on closing communications or cases in closed status
Y. Completion and Submission of the FD-930
1. Completion of Gang, Subgroup, and File # fields
a) In the Gang field, enter "International Extremist"
b) In the Subgroup field, enter the VGTOF handling code (1, 2, 3, 4, or silent hit)
c) In the File # field, enter the substantive 288J file number, not an administrative file number (such as the 66 classification) or other control file number
2. To remove or modify a record in VGTOF, send a copy of the closing communication and an enclosed FD-930 to the [redacted] Check the "Remove" box or the "Supplements Initial Submission" box at the top of the form. The FD-930 must be sent directly to the [redacted] not to the substantive unit. b7E
3. All subjects of Preliminary Investigations must be removed from VGTOF and other watch lists when the case is closed.
4. Subjects of Full Investigations may remain in VGTOF and other watch lists, if appropriate. Example: The subject of a Full Investigation is still a threat to national security, but moves to another field office's area of responsibility or outside the USA and thus the field office closes its case. Notify appropriate field office or Legat in the Details area of the closing communication
Z. (U) The Behavioral Analysis Program
1. (U) See: Section 2-35, supra.

Section 23-14 (U) 288L - Technical Support to International Terrorism Matters

A. General
1. (U) Technical Support to International Terrorism investigations are conducted in support of the FBI's priority to protect the United States from terrorist attack with the goal of preventing, disrupting, and defeating terrorist operations before they occur. The purpose of these investigations is to provide expert technical assistance in international terrorism investigations, when the basis for the international terrorism investigation does not warrant opening a Preliminary Inquiry or Full investigation under the 288J classification.
B. Authorities and Requirements in Technical Support to International Terrorism Matters
(U) 1. (X) Authority for conducting the investigative techniques in a 288L Technical Support investigation rests with the squad supervisor. b7E
(U) 2. (X) A 288L technical support investigation may only be opened in support of an authorized [redacted]
(U) 3. (X) Unlike 288J classification reporting requirements for Preliminary Inquiry and Full investigations, a technical support investigation does not have specific reporting requirements.

[redacted]

b7E

(U) 4. (~~S~~) Significant Investigative Milestones- major investigative steps shall be provided to FBIHQ by an official communication on a timely basis when they occur, irregardless of other reporting requirements.

(U) 5. (~~S~~) Investigations under the 288L classification must be closed before or at the same time as the corresponding international terrorism matter.

Section 23-15 (U) Relevant Statutes

18 U.S.C. § 1030. Fraud and related activity in connection with computers
(a) Whoever--
(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;
(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains--
(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);
(B) information from any department or agency of the United States; or
(C) information from any protected computer if the conduct involved an interstate or foreign communication;
(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;
(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;
(5)(A)(i) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;
(ii) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or
(iii) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage; and
(B) by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused (or, in the case of an attempted offense, would, if completed, have caused)--
(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related

course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;
(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;
(iii) physical injury to any person;
(iv) a threat to public health or safety; or
(v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security;
(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if--
(A) such trafficking affects interstate or foreign commerce; or
(B) such computer is used by or for the Government of the United States; [FN1]
(7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer; shall be punished as provided in subsection (c) of this section.
(b) Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.
(c) The punishment for an offense under subsection (a) or (b) of this section is--
(1)(A) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and
(B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;
(2)(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), (a)(5)(A)(iii), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;
(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2), or an attempt to commit an offense punishable under this subparagraph, if--
(i) the offense was committed for purposes of commercial advantage or private financial gain;
(ii) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or
(iii) the value of the information obtained exceeds $5,000; and
(C) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;
(3)(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and
(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4) [FN2] (a)(5)(A)(iii), or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;
(4)(A) except as provided in paragraph (5), a fine under this title, imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(5)(A)(i), or an attempt to commit an offense punishable under that subsection;

(B) a fine under this title, imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(5)(A)(ii), or an attempt to commit an offense punishable under that subsection;
(C) except as provided in paragraph (5), a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(A)(i) or (a)(5)(A)(ii), or an attempt to commit an offense punishable under either subsection, that occurs after a conviction for another offense under this section; and
(5)(A) if the offender knowingly or recklessly causes or attempts to cause serious bodily injury from conduct in violation of subsection (a)(5)(A)(i), a fine under this title or imprisonment for not more than 20 years, or both; and
(B) if the offender knowingly or recklessly causes or attempts to cause death from conduct in violation of subsection (a)(5)(A)(i), a fine under this title or imprisonment for any term of years or for life, or both.
(d)(1) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section.
(2) The Federal Bureau of Investigation shall have primary authority to investigate offenses under subsection (a)(1) for any cases involving espionage, foreign counterintelligence, information protected against unauthorized disclosure for reasons of national defense or foreign relations, or Restricted Data (as that term is defined in section 11y of the Atomic Energy Act of 1954 (42 U.S.C. 2014(y)), except for offenses affecting the duties of the United States Secret Service pursuant to section 3056(a) of this title.
(3) Such authority shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.
(e) As used in this section--
(1) the term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device;
(2) the term "protected computer" means a computer--
(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or
(B) which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States;
(3) the term "State" includes the District of Columbia, the Commonwealth of Puerto Rico, and any other commonwealth, possession or territory of the United States;
(4) the term "financial institution" means--
(A) an institution, [FN3] with deposits insured by the Federal Deposit Insurance Corporation;
(B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;
(C) a credit union with accounts insured by the National Credit Union Administration;
(D) a member of the Federal home loan bank system and any home loan bank;
(E) any institution of the Farm Credit System under the Farm Credit Act of 1971;
(F) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934;
(G) the Securities Investor Protection Corporation;
(H) a branch or agency of a foreign bank (as such terms are defined in paragraphs (1) and (3) of section 1(b) of the International Banking Act of 1978); and
(I) an organization operating under section 25 or section 25(a) of the Federal Reserve Act;

(5) the term "financial record" means information derived from any record held by a financial institution pertaining to a customer's relationship with the financial institution;
(6) the term "exceeds authorized access" means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter;
(7) the term "department of the United States" means the legislative or judicial branch of the Government or one of the executive departments enumerated in section 101 of title 5;
(8) the term "damage" means any impairment to the integrity or availability of data, a program, a system, or information;
(9) the term "government entity" includes the Government of the United States, any State or political subdivision of the United States, any foreign country, and any state, province, municipality, or other political subdivision of a foreign country;
(10) the term "conviction" shall include a conviction under the law of any State for a crime punishable by imprisonment for more than 1 year, an element of which is unauthorized access, or exceeding authorized access, to a computer;
(11) the term "loss" means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service; and
(12) the term "person" means any individual, firm, corporation, educational institution, financial institution, governmental entity, or legal or other entity.
(f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.
(g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in clause (i), (ii), (iii), (iv), or (v) of subsection (a)(5)(B). Damages for a violation involving only conduct described in subsection (a)(5)(B)(i) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.
(h) The Attorney General and the Secretary of the Treasury shall report to the Congress annually, during the first 3 years following the date of the enactment of this subsection, concerning investigations and prosecutions under subsection (a)(5). 18 U.S.C. § 2703. Required disclosure of customer communications or records
(a) Contents of wire or electronic communications in electronic storage.--A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.
(b) Contents of wire or electronic communications in a remote computing service.--(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection--

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant; or
(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity--
(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or
(ii) obtains a court order for such disclosure under subsection (d) of this section; except that delayed notice may be given pursuant to section 2705 of this title.
(2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service--
(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and
(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.
(c) Records concerning electronic communication service or remote computing service.--(1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity--
(A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant;
(B) obtains a court order for such disclosure under subsection (d) of this section;
(C) has the consent of the subscriber or customer to such disclosure;
(D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title); or
(E) seeks information under paragraph (2).
(2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the--
(A) name;
(B) address;
(C) local and long distance telephone connection records, or records of session times and durations;
(D) length of service (including start date) and types of service utilized;
(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and
(F) means and source of payment for such service (including any credit card or bank account number), of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).
(3) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.
(d) Requirements for court order.--A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. In the case of

a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

(e) No cause of action against a provider disclosing information under this chapter.--No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, statutory authorization, or certification under this chapter.

(f) Requirement to preserve evidence.--

(1) In general.--A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

(2) Period of retention.--Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90- day period upon a renewed request by the governmental entity.

(g) Presence of officer not required.--Notwithstanding section 3105 of this title, the presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber to or customer of such service.

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 5
Page 6 ~ b1, b7E
Page 7 ~ b1
Page 11 ~ b1
Page 15 ~ b1
Page 19 ~ b1, b7E, Referral/Consult